Методичка 2.1 - Базовые знания

Системы счисления

В обычной жизни мы используем десятичную систему счисления. Для человека она является основной. Называется она десятичной, потому что в ней используются 10 цифр: от 0 до 9. Существуют и другие системы счисления, например, двоичная, троичная, восьмеричная.

Процессор работает с двоичной системой счисления, которая содержит только 2 цифры: 0 и 1. Двоичную систему выбрали не случайно, дело в том, что процессор состоит из множества транзисторов, на которые подается напряжение. И получается, что очень легко можно сопоставить состояние, когда есть напряжения и когда нет. Когда напряжения нет - это 0, а когда есть - это 1. Это конечно, сильно упрощенное объяснение, но вполне подойдет для общего понимания.

Процессоры работают с двоичной системой счисления. Каждая цифра в двоичном числе называется битом. 8 бит называется байтом, 16 бит - это слово, 32 бита - это двойное слово. Нумерация бит в двоичном числе начинается с нуля и отсчет идет справа налево. Справа находятся младшие биты, слева - старшие. Для того, чтобы указать, что число представлено в двоичной системе, необходимо в конец добавить букву b. Например, 10b.

При разработке программ на языке Ассемблер мы будем использовать шестнадцатеричную систему счисления. Принцип такой же, только в отличие от десятичной в ней используется 10 цифр и 6 букв. Цифры от 0 до 9 и буквы от A до F. Для того, чтобы указать, что число представлено в шестнадцатеричной системе, необходимо в конец добавить букву h. Например, 10h. Также допускается перед числом указать 0x, например, 0xAAFF.

Для перевода из одной системы счисления в другую существуют специальные формулы, познакомиться с ними можно по ссылке, которая представлена ниже:

Ссылка: http://inf.e-alekseev.ru/text/Schisl_perevod.html

В курсе для перевода из одной системы счисления в другую будет использоваться стандартный калькулятор Windows.

Для этого необходимо открыть калькулятор. Перейти в режим - Программист. После этого появится выбор систем счисления:

Hex - шестнадцатеричная
Dec - десятичная
Oct - восьмеричная
Bin - двоичная

Если необходимо перевести число из десятичной системы в шестнадцатеричную, то необходимо выбрать Dec, ввести число, например, 200, и переключиться на Hex. Представление числа должно измениться на 0xC8.

Если необходимо перевести число из шестнадцатеричной системы в двоичную, то необходимо выбрать Hex, ввести число, например, AF, и переключиться на Bin. Представление числа должно измениться на 10101111b.

Рекомендации по установке среды разработки Visual Studio

Ссылка: https://visualstudio.microsoft.com/ru/downloads/

Следует выбрать при установке следующие компоненты:

Desktop Development with C++
- C++ Core Desktop Features
- MSVC v142
- Windows 10 SDK
- Just-In-Time debugger

Visual Studio включает в себя не только транслятор MASM, но и компилятор Visual C++, который понадобится в будущих уроках этого курса.

Компиляция программы

(1 мин.)

Исходный код программы prog-1.1.asm

```
.386
.model flat, stdcall

_data segment
message db 'Hello, World!',0
_data ends

_text segment
start:
xor eax, eax
add eax, 4
inc eax
ret
_text ends
end start
```

Трансляцию программы необходимо выполнить через командную строку Visual Studio с помощью транслятора MASM. Командную строку Visual Studio можно найти через меню Пуск. Нам необходим командная строка для создания программы под архитектуру x86.

Трансляция программы - это процесс перевода команд на языке Ассемблер в опкоды, которые понимает процессор.

Трансляция:

```
> ml /c /coff prog-1.1.asm
```

```
> ml /help
```

Параметр /c - выполнить только трансляцию без линковки.

Параметр /coff - создать объектный файл в формате COFF (Common Object File Format).

После трансляции получаем объектный файл prog-1.1.obj. Для того, чтобы запустить программу в Windows необходимо выполнить линковку (компоновку) программы.

Линковка - это процесс создания исполняемого файла, в котором будут объединены указанные объектные файлы и созданы все необходимые связи, а также добавлен PE-заголовок, который необходим загрузчику при запуске программы.

Линковка:

```
> link /SUBSYSTEM:CONSOLE prog-1.1.obj
```

Посредством параметра SUBSYSTEM задаем тип приложения: консольное или с графическим интерфейсом. Если указываем при линковке CONSOLE, то при запуске такого приложения сначала запустится командная строка и в ней запустится приложение. Если указываем WINDOWS, то приложение будет запускаться напрямую, без командной строки.

После линковки получаем исполняемый файл prog-1.1.exe.

Запуск:

```
> prog-1-1.exe
```

Программа запустилась, что-то сделала и завершилась. Для того, что посмотреть на ее структуру можно воспользоваться утилитой dumpbin.

```
> dumpbin /ALL prog-1.1.exe
```

Microsoft (R) COFF/PE Dumper Version 14.22.27905.0
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file prog-1.1.exe

PE signature found

File Type: EXECUTABLE IMAGE

FILE HEADER VALUES

14C	machine (x86)
3	number of sections
5D45B00C	time date stamp Sat Aug 3 09:02:20 2019
0	file pointer to symbol table
0	number of symbols
E0	size of optional header
102	characteristics
	Executable
	32 bit word machine